10th Symposium on Privacy and Security
ETH Zurich

Information Security 2015

Paul C. Van Oorschot

Digital Security Group
School of Computer Science
Carleton University, Ottawa, Canada

1 September 2005

1

System Integrity vs. Transaction Security [OVERVIEW]

Internet security technologies generally fall into two classes:

A. System Integrity
- ~ safe roads to drive on (infrastructure; pathways)
- counters: vandalism, seizing control of resources

B. Transaction Security
- ~ safe vehicles to carry goods (data; transactions)
- counters: data theft, fraud, impersonation, improper access
- supports: privacy, accountability of business transactions

☞ A is ultimately harder to guarantee; but necessary for B

2

Selected Pieces of Internet Security Puzzle

A. System Integrity	B. Data/Transaction Security
• DNS • secure routing (BGP) • firewalls & filtering • hardened systems • access control (O/S) • audit trails & logs • patching & updating • software protection • anti-virus • IDS & scanning tools • anti-DDoS tools	• SSL (session protection) • crypto, persistent encryption,... • strong authentication • secure remote access, VPNs • PKI / identity management • PMI / authorization • secure payment and banking • privacy • . . .

3

Paradigm Shifts in Computing [↑ SECURITY CHALLENGES]

1. mainframe
2. workstations/PC's + LANs
3. client-server + gateways to external networks
4. [full] Internet connectivity (global, wireline)
5. → wireless + mobile computing + "anywhere" remote access
6. pervasive computing (interconnected embedded devices)

Add: constantly evolving software/threats from:

- traditional software feature upgrades
- ubiquitous active content downloads
- auto-updates • P2P activity • worms, viruses, spyware

2015:

No one pretends to know what software is running on their machine

4

The ID-Theft Game: Players & Motives

- private citizen + credential issuer + relying party
- authorized data holders (employer, banks, government)
- credit bureaus + data brokers
- attackers

Motives of each player are some combination of:

1. to protect and selectively provide data
2. to share/sell data (or a function thereof) ←
3. to properly verify credentials
4. to steal/exploit data

☞ Compare: "simple" 2- and 3-party crypto protocol theory

2015:

For-fee "identity protection services" are profitable, commonly used

5

Phishing & Key Logging

phishing kits available on Internet

- to create bogus websites, and use spamming software

key logging – e.g., trojan Bankhook.A (June 2004)

- spreads by browsing; exploits IE vulnerability
- on detecting connect attempts to any of 50 online banks, records sensitive info pre-SSL, mails to remote computer
- alternative: hardware token key-logger

2015:

- *"techno-social engineering" issues still evade technical solutions*
- *many new issues (address resolution: pharming, bookmarks, ...)*

6

Trustworthiness of User Interface

- today's Internet footprint (browser UI) is not trustworthy
  - secure GUI is extremely hard problem
- users are a weak link (beyond passwords)
  - increasingly complex systems, inexperienced users
  - no time, interest, ability to learn
- astounding lack of human factors design & research in security

2015:

- *recognition: commodity PC's can't provide usable + secure UI*
- *Internet access is 2-tier: commodity, trustworthy devices*
- *higher-value services available only to 2nd-tier devices*

7

Example of Changing Rules: Cryptographic Assumptions

Fundamental cryptographic assumption:
- end-points are secure (→ secret key is safe)

Current Internet environment:
- client environments untrusted (malware)

→ must re-examine fundamental assumption

2015:

- *cleartext over Internet links is rare (unacceptable in business)*
- *persistent protection is major focus*
- *DRM remains challenging; "electronic originals" technology in use*

8

Computer Worms

- Slammer (Jan. 2003): single-packet UDP worm [non-malicious]*
  - 90% of vulnerable hosts infected in 10 min
  - scanning rate: 55M scans/sec after 3 minutes
- hit-lists and flash worms (10's of seconds)
  - attack speed vs. limits of human intervention
- mass-mailing worms; IM worms

2015:

- *new forms of malware continue to arise, evolve*
- *diversity, obfuscation embraced by attackers*
- *past lessons remain unlearned (cf. Morris worm 1988)*
- *specialized devices (cells, VoIP, ...) subject to worms, spam, . . .*

9

Botnets

- IRC: 1-to-many real-time communication
- typical botnet: compromised PCs managed over IRC channel
  - typically up to 10,000 machines; 50,000+ observed
- ex: 1000 PC's, average upstream 128KBit/s = 100MBit/s+
  - distribution of IP addresses makes filtering difficult
- DDoS, spam, phishing, bootstrapping spread of malware
  - ex: 3-10 cents / host / week for SPAM proxying

2015:

- *botnets viewed as having been a very significant evolutionary step*
- *↑ economically-motivated malware: organized crime, espionage*
- *Internet taxed to subsidize real-world pursuit of cyber-criminals*

10

Software: A Very Weak Link

- price of software + pace of change
  - application developers building brick houses on quicksand
- monoculture (O/S, applications, protocols, standards)
- language-based and memory-related exploits
  - still largely unaddressed in undergrad curricula

2015:

- *100's of millions of lines of C code remain in commercial use*
- *buffer overflow (related) problems remain far from solved*

2015:

- *value of diversity is broadly recognized*
- *interoperability recognized to have significant -ve component*

11

IP Convergence

- IP convergence trend (e.g., VoIP): unstoppable; driven by $
- trend to totally "open" systems

2015:

- *businesses must still support non-IP phones*
- *many customers save $, but telecoms don't*
- *robustness of voice network decreases dramatically (openness)*

12

Formal Analysis and Provable Security

- "proofs" of security vs. real-world guarantees
  - assumptions and models rarely match real world
    (. . . even before considering software vulnerabilities)
- analysis tools promote "useful thinking"

2015:

- *large gaps remain between theoretical research & practical security*
- *practical confidence still from: experience; soak-time; trial & error*

13

Other Business & Legal Issues

2015:

Possibilities:

1. enterprises liable for malicious outbound connections
   - IDS goals change
2. vendors liable for bad software
   - executives accountable for s/w shipped with known bugs (cf. autos)
   - valuations hurt; many small players fail
3. insurance rates depend on O/S and applications used
4. stronger domestic, international laws: limited success
   - jurisdictional issues (non-resident attackers)
   - "DMCA problem"

14

2015:

The Internet in 2015: World #1

"Max Max" Internet

[functionality continues ↑, and/or security issues not addressed]:

- malware becomes part of the eco-system
  - competition for desktop resources; a battle to maintain its integrity
  - computers are untrusted; perhaps some programs trusted
- Internet viewed as "disposable"; disposable clients
- regular Internet outages due to attacks on critical infrastructures
  - hijacked IP addresses (BGP), poisoned DNS tables, . . .
- many users abandon email
- e-commerce dies; Internet mainly used for publishing info cheaply

15

2015:

The Internet in 2015: World #2

"Business" Internet

[functionality is constrained; security ↑]

- stronger authentication, accountability, traceability
- widespread support for "private numbers" (email, web sites)
- tradeoffs made (e.g., anonymity), where necessary for ↑ security
- extreme case: fixed-functionality, specialized clients (no software)
- still no global PKI
  - "blind man does business with stranger in foreign land"
  - communities of trust

16

Concluding Remarks

- need more tools to detect ongoing mal-access (vs. intrusions in progress)
- engage enemy/maintain contact vs. blindly reinforcing perimeters
  - learn more; remove root causes
- terrible defensive track record vs. emergent Internet threats
  - 0-day worms, DDoS, large-scale spam, ID theft, botnets, . . .

17

2005 Security Scorecard (personal view)

• crypto:	A/C-	(technology / deployment)
• viruses:	B	(updates; zero-day; social engineering)
• firewalls:	C	(configuration; http tunneling)
• spam:	C-	(spoofed From; 0wned machines)
• PKI:	D	(interoperability; deployment; usability)
• IDS:	D	(false +/-ve; log monitoring ($); detect-only)
• worms:	D	(progress since 1988? “gaming” → DoS)
• DDoS/NDoS:	D	(hard to win an asymmetric war)
• passwords:	D/A	(technology / deployment; here to stay)

18

Thank you

Paul C. Van Oorschot

Digital Security Group
School of Computer Science
Carleton University, Ottawa, Canada

19